中央銀行から見たブロックチェーン技術の可能性とリスク

日本銀行
決済機構局 FinTechセンター長
審議役
岩下 直行 氏

2016年11月、日本IBM本社で、「Blockchain Summit 2016」を開催しました。このサミットの基調講演として行われた、日本銀行 決済機構局 FinTechセンター長 審議役 岩下直行氏の講演をご紹介します。ブロックチェーンの歴史を振り返った上で、ブロックチェーンがどのような可能性を持った技術かを理解することで、今後の発展、応用の可能性を考えることができます。

ブロックチェーンの分野は急速な進化を遂げています。我々も必死で最新動向を追いかけていますが、日本銀行として公式見解をまとめるまでには至っていません。今回の講演はあくまでも私見であり、日本銀行としての公式的な見解ではないことをはじめにお断りしておきます。

ビットコイン誕生以前の電子現金

まず、ビットコインの歴史を振り返っておきたいと思います。「ビットコインは、ブロックチェーン技術によって作られた仮想通貨の一つ」と紹介されることがありますが、歴史的には、最初にビットコインが存在し、そこからブロックチェーンが誕生し、さらにDLT（Distributed Ledger Technology：分散台帳技術）が生まれたという順番です。

ビットコイン誕生以前から、電子現金（Electronic Cash）の技術は存在していました。1992年に誕生したSurety社の「Digital Notary」は、ハッシュ値を連鎖させることで電子的なタイムスタンプ性を実現するサービスで、その連鎖の一部をニューヨーク・タイムズ紙に掲載することで、信頼性を確保するという工夫をしていました。また、1994年に誕生したDigicash社の「ecash」は、「blind signature」という暗号技術を使い、取引の匿名性を実現したclosed-loop型の電子現金です。

つまり、ビットコインの誕生前から、ビットコインの特徴である「乱数とデジタル署名を用いた電子現金」「分

割可能性、open-loop性、匿名性の付与」「ハッシュ関数や署名の連鎖による改ざん防止」についてさまざまな技術が考案され実装されていたということです。その中には、今でいう「仮想通貨的なもの」も多数存在しましたが、注目されずに消滅しました。利用するコンピューター側のシステムリソースの不足やコスト、利便性の問題などから、当時はそれらの技術が広く普及することがなかったのです。

なぜビットコインは成功したのか

ビットコインは、2008年にSatoshi Nakamotoが発表した論文で紹介され、2009年1月に「Bitcoin v0.1」がリリースされました。このSatoshi Nakamotoを名乗る人物は、その後表舞台から姿を消し、残った仲間がビットコインの開発を続けていきます。

ビットコインは発行主体を持たず、インターネット上のピア・ツー・ピア（P2P）ネットワークで情報が共有されます。誰でも利用者となることができ、ソースコードや取引履歴の検証を可能とすることで、信頼性を確保しています。計算能力を提供してシステム全体の維持管理に貢献する「発掘＝マイニング」に対して、一定の報酬が与えられます。この報酬を求めて、専門業者が膨大な計算能力を投入してマイニングを進めています。このマイニングの仕組みこそが、単にハッシュ値をたくさん計算して正解を見つける競争にとどまらず、ビットコインの安全性を実現する要因になっています。

ビットコインの交換価値は変動があったものの、現在は700ドルから800ドルをうかがう状況にあります。また注目すべきは、グローバルでの利用者数が2016年11月時点で1,000万人に迫る規模となっていることです（**図1**）。

あらためてビットコインが成功した理由を考えてみたいと思います。

1つは、P2Pによる分散コンピューティングを採用したことです。ビットコイン誕生前史にもさまざまな取り組みや仮想通貨的なものが開発されましたが、それらは運用を行うセンターシステムが必要で、それを維持するために多くのコストがかかっていました。一方、P2P方式を採用したビットコインにはセンター維持コストが必要なく、さらに、CPU、ストレージ、通信のコストが下がったことで、一般ユーザーが保有するインターネット上のリソースだけで稼働可能となりました。

2つ目は、マイニングに対して報酬付与を行うことで、ビザンチン障害耐性を獲得したことです。分散コンピューティングにすることで、嘘をついたり悪いことをしたりする人がいたとしても、それを駆逐することができるシステムの頑健さを手に入れました。

3つ目は、独自通貨単位である「BTC」を採用したことです。単に決済手段として使うのであれば、日本の円や米国ドルといった法定通貨建ての方が使いやすいわけですが、BTCの採用により投資機会を提供し、株式のように投機的資金も流れ込むようになりました。マイニングの報酬分だけBTCを追加発行すればよく、外部からの費用投入なしにシステムを維持することができます。このようにシステム維持費用を自給自足できる仕組みを構築できたことが、ビットコインが現在成功している一因と考えられます。

ただし、国際決済銀行 決済・市場インフラ委員会が発

図1. ビットコインの価格と利用者数の推移

行した「デジタル通貨報告書 <2015>」には、次のような指摘があります。

「デジタル通貨は特定の個人や機関の負債ではなく、当局による裏付けもない。さらに、本源的価値はゼロであり、結果的に、その価値は他の財・サービスないしソブリン通貨に後日交換されるという信頼にのみ由来する。したがって、デジタル通貨の保有者のほうがソブリン通貨の所有者よりも、価格変動・流動性リスクに起因するコストや損失に直面する可能性が高い。」

このような指摘も念頭に置いておいた方がよいでしょう。

ブロックチェーンとDLT

ビットコインが注目を集め、類似の技法で新たな仮想通貨が開発されるようになると、技術面に着目したそれらの総称として「ブロックチェーン」という言葉が使われるようになりました。また、その技術が仮想通貨以外にも適用されるようになると、ブロックチェーンという言葉よりも汎用的な印象のある「DLT」という用語が使われるようになりました。

ブロックチェーンとDLTの定義については、さまざまな議論が行われています。現段階では広く合意された定義があるわけではなく、ビットコインとは異なるイメージで捉えたい場合は、ブロックチェーンという言葉に代えてDLTと呼称することもあります。

例えば、日本ブロックチェーン協会（JBA）では、狭義、広義のブロックチェーンの定義を提示しています。

狭義のブロックチェーン：「ビザンチン障害を含む不特定多数のノードを用い、時間の経過とともにその時点の合意が覆る確率が0へ収束するプロトコル、またはその実装を『ブロックチェーン』と呼ぶ。」

広義のブロックチェーン：「電子署名とハッシュポインタを使用し改竄検出が容易なデータ構造を持ち、且つ、当該データをネットワーク上に分散する多数のノードに保持させることで、高可用性及びデータ同一性等を実現する技術を『広義のブロックチェーン』と呼ぶ。」

この広義と狭義の差の部分がDLTだという考え方もあります。こうした分類法とは別に、プライベート型、パブリック型という分け方があります。さらにそこにコンソーシアム型を入れて、3つに分類することもあります（**図2**）。

プライベート型は単独機関が管理し、ノード参加者は管理者による許可制、合意形成は厳格でなくても可能で、取引速度は高速です。パブリック型は、管理者が存在せず、ノード参加者には特に制限がありません。合意形成は厳格である必要があり、取引速度は低速になります。コンソーシアム型は、管理者は複数のパートナーによるもので、ノードに参加するためには管理者による許可が必要です。合意形成は厳格ではないことが可能で、取引速度は高速です。日本銀行はプライベート型を考えているだろうと思われるかもしれませんが、決してそんなことはありません。パブリック型、コンソーシアム型を含めて評価をしています。

大きな流れとしては、現在、金融業界が実証実験のターゲットとしているのがプライベート型やコンソーシアム型です。パブリック型はビットコインなどの仮想通貨の基盤として利用されています。

現在の金融業界では、「パブリック型は危ないが、プライベート型やコンソーシアム型のブロックチェーンなら大丈夫」という考え方がありますが、私はそれには少し疑問を感じています。パブリック型の合意形成の仕組みを上手く使えば、これまでになかったソリューションができるのではないかという大きな可能性を感じています。また、コンソーシアム型において高速で厳格でない合意形成を行うとき、コンセンサスのアルゴリズムのあり方について実はまだいろいろな議論があり、これからの技

	プライベート型	コンソーシアム型	パブリック型
管理者	単独の機関	複数のパートナー	存在せず
ノード参加者	管理者による許可制	管理者による許可制	制限なし
合意形成	厳格ではないことが可能	厳格ではないことが可能	厳格であることが必要（PoW、PoS等）
取引速度	高速	高速	低速

図2. ブロックチェーンの3つの型

技術の使い方／分野	金融	産業	行政	CivicTech
1.ビットコインなどを仮想通貨としてそのまま使う	国際送金	貿易金融	社会保障支払の改善、国際援助の透明化	
2.ビットコインなどの元帳機能のみを利用する	証券ポストトレード	サプライ・チェーン		学位認定、臨床試験の研究記録
3.オリジナルの分散元帳を構築する	銀行勘定系システムの構築、証券ポストトレード、小切手の電子化、KYC/AML	サプライ・チェーン	知財管理、ヘルスケア、消費税徴税事務の改善	土地登記、法人登記

図3. ブロックチェーンのユースケース

術開発が必要になるだろうと思っています。

ブロックチェーンのユースケースとしては、金融分野ではもちろん、産業界、行政、さらには市民のさまざまなアクティビティーに関わるCivic Tech[※1]の分野においても活用が考えられます（**図3**）。例えば、行政における仮想通貨としてのユースケースとして、発展途上国や紛争が起きている国へ国際援助を行う際に仮想通貨を使えば、援助すべき相手に資金を送ったかを確認することができる、といった利点を生かすことが考えられます。

※1 シビック（Civic：市民）とテック（Tech：テクノロジー）をかけあわせた造語。市民自身が、テクノロジーを活用して、行政サービスの問題や社会課題を解決する取り組みをいう。

ブロックチェーン2.0とThe DAO事件

最近、「ブロックチェーン2.0」と呼ばれる新サービスが次々に登場しています。

「スマート・コントラクト」は契約書をブロックチェーンに載せることで契約を執行させる機能を持たせたものです。また、「スマート・プロパティ」は、資産・契約書をブロックチェーンに載せたもので、契約を執行させる機能はありません。DAO（Decentralized Autonomous Organization：自律分散型組織）もそうした新しいサービスの一つです。分散型自動化組織で、スマート・コントラクトをさらにまとめて、自動執行するようにしたものです。

このDAOの有効性を示すために、IoTを活用したシェアリング・エコノミーの展開を目指す「The DAO」という事業ファンドがEthereum[※2]というブロックチェーン上に誕生し、1カ月弱の間に1万1,000人の投資家から156億円を調達しました。しかし、その資金が攻撃にあい、50億円が抜き取られる事態が起こりました。この事件から学ぶべき教訓は多く、既成の法制度に頼らない分散型の合意形成の仕組みが有用であるとしても、制度設計やシステム設計にはさらなる検討が必要だということです。また、問題発生と対応の課程で、スマート・コントラクトやブロックチェーンによる価値の保有そのものの問題点も明らかになりました。

こうした課題を抱えつつも、IoTと連動したFinTechの取り組みは有望視されており、さらなるチャレンジが予想されています。

※2 イーサリアム・プロジェクトにより開発が進められている、分散型アプリケーションやスマート・コントラクトを構築するためのプラットフォームの名称、および関連するオープンソース・ソフトウェア・プロジェクトの総称。

ブロックチェーンと中央銀行

各国の中央銀行は、ブロックチェーンやデジタル通貨に強い関心を持っています。その理由は、デジタル通貨には、銀行券や銀行預金にはない強みがあるからです。

現在の銀行券は、偽造防止技術を盛り込んでいますが、アンチ・マネー・ロンダリング（AML）に対して対応困難です。銀行預金は、個人認証と勘定系技術をベースにしているため、AMLには強い反面、匿名性が低いという課題を持っています。しかしデジタル通貨は、ブロックチェーン技術をベースに、AMLに対応することも、プライバシー保護に対応することもできます。銀行券、銀行預金の強み、弱みをカバーする存在になる可能性があるのです（**図4**）。

日本銀行では2016年4月に「FinTechセンター」を設立しました（**図5**）。これまで金融機構局、決済機構局、金融研究所、さらにその他の関係局がそれぞれやってきたことをまとめ、新しい時代に対応することを目指した検討体制を構築しました。日本銀行は、日本円をより強力で便利なものにするために、積極的に活動していきたいと考えています。

	基盤となる技術	AML	プライバシー保護	受け渡しにおける第三者の関与
銀行券	偽造防止技術	対応困難	対応不要	不要
銀行預金	個人認証 ＋ 勘定系	対応可能	対応困難	必要
デジタル通貨	ブロックチェーン技術	対応可能	対応可能	不要

図4. 銀行券、銀行預金、デジタル通貨の比較

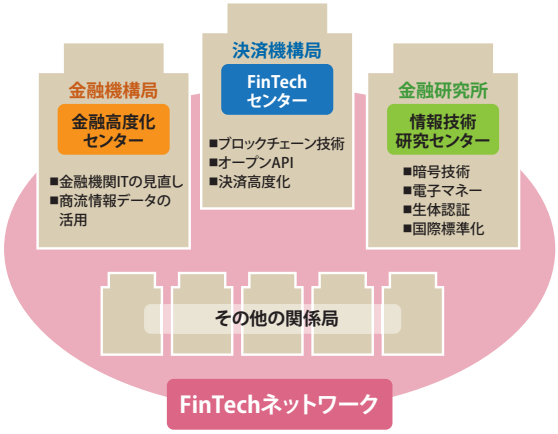

図5. 日本銀行のFinTech検討体制